Appl. No. 10/782,751
Amdt. dated April 14, 2008
Reply to Office Action of October 17, 2007

PATENT

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1-2. (Canceled).

3. (New)   A method for reprovisioning a token having a first secret, comprising:

sending a request for a certificate;

receiving a certificate that contains a second secret encrypted with a public key of the token, the second secret distinct from the first secret;

decrypting the second secret with a private key of the token; and

generating a one time password based on the second secret.

4. (New)   The method of claim 3, further comprising, subsequent to receiving the second secret, discontinuing generation of one time passwords based on the first secret.

5. (New)   The method of claim 3, wherein the second secret is a symmetric cryptographic key.

6. (New)   The method of claim 3, wherein the one time password based on the second secret is further based on a personal identification number.

7. (New)   The method of claim 3, wherein the one time password based on the second secret is further based on a signal from a clock.

8. (New)   The method of claim 3, wherein the one time password based on the second secret is further based on a counter value.

Appl. No. 10/782,751
Amdt. dated April 14, 2008
Reply to Office Action of October 17, 2007

PATENT

9. (New)   A token for generating one time passwords, comprising:

a processor; and

a memory coupled to the processor, the memory storing a first secret and token instructions adapted to be executed by the processor to send a message that includes a request for a certificate, receive a certificate that includes a second secret encrypted with a public key, decrypt the second secret with a private key of the token, store the second secret in memory, and generate a one time password based on the second secret.

10. (New)   The token of claim 9, further comprising, subsequent to receiving the second secret, discontinuing generation of one time passwords based on the first secret.

11. (New)   The token of claim 9, wherein the second secret is a symmetric cryptographic key.

12. (New)   The token of claim 9, wherein the token instructions are further adapted to be executed by the processor to generate the one time password based on a personal identification number.

13. (New)   The token of claim 9, wherein the token instructions are further adapted to be executed by the processor to generate the one time password based on the second secret and a time value.

14. (New)   The token of claim 9, wherein the token instructions are further adapted to be executed by the processor to generate the one time password based on the second secret and a counter value.